UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,899	08/10/2001	R. David L. Campbell	KANG115519	5461

26389 7590 07/09/2007
CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
LEROUX, ETIENNE PIERRE	

ART UNIT	PAPER NUMBER
2161	

MAIL DATE	DELIVERY MODE
07/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/927,899
Filing Date: August 10, 2001
Appellant(s): CAMPBELL ET AL.

D. C. Peter Chu
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/22/2007 appealing from the Office action mailed 4/19/2005

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,968,176	Nessett et al	10-1999
2002/0129058	Story et al	9-2002
6,539,021	Kennelly et al	3-2003

6,339,826	Hayes et al	1-2002
5,946,686	Schmuck et al	8-1999

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 6-8, 10, 22 and 23 are rejected under 35 U.S.C. 102(e) as being anticipated by US Pat No 5,968,176 issued to Nessett et al (hereafter Nessett).

Claims 6, 22 and 23:

Nessett discloses a method for providing remote access to the facilities of a server computer, comprising:

receiving a request [Fig 2, 111,col 10, lines 40-45] at a server computer [Fig 2, 115] operative to store and update a network database to add a new user to a group of users authorized to utilize said network database [col 15, lines 40-45];

determining whether said request may be granted [col 15, lines 40-55];

in response to determining that said request may be granted, adding said new user to said group of users authorized to utilize said network database [Fig 2 and col 16, line 55 through col 17, line 3, group membership], the said group of users defining a collaborative group spanning across the server computer and another server computer so as to allow users to share data [groups of user identifiers, col 8, lines 27-34, col 16, line 60 through col 17, line 5, group membership].

Claim 7:

Nessett discloses wherein said request is received over a secure communications link from a second server computer [col 16, lines 13-20].

Claim 8:

Nessett discloses wherein a login and password for said new user are provided as a part of said request [col 12, lines 10-21].

Claim 10:

Nessett discloses wherein said server computer comprises a server computer operative to store and update a network database, and wherein said second server comprises a server computer operative to provide an Internet Web site [Fig 2 and col 15, lines 40-47].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Pat No 5,968,176 issued to Nessett et al (hereafter Nessett) in view of Pub No US 2002/0129058 issued to Story et al (hereafter Story).

Claim 1:

Nessett discloses a method for providing remote access to the facilities of a server computer, comprising:

receiving a user request [Fig 2, stand alone dial-up end system 111] to access a first server computer [Fig 2, line server 104];

determining whether said user request may be granted [user authentication, col 15, lines 40-55];

in response to determining that said user request may be granted, determining whether access to a second server computer [Fig 2, packet server 108, split service access, col 15, lines 55-65, sharing access, col 18, lines 20-25] should also be granted;

in response to determining that access to said second server computer should be granted transmitting a request to access to said second server computer from said first server computer to said second server computer via a secure communications connection [col 15, lines 55-65 and col 16, lines 13-20, cryptographic protocols that run over serial lines].

Nessett discloses the elements of the claimed invention as noted above but does not disclose said second server computer is operative to provide facilities for storing and updating said network database in a manner that is visually consistent with a Web site on the first server. Story discloses said second server computer is operative to provide facilities for storing and updating said network database in a manner that is visually consistent with a Web site on the first server [paragraph 53, documents in stage directory 64 may be distributed to a directory on network server 62, Fig 6, company logos are stored on a logo directory, each hypermedia document references the documents in the logo directory]. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nessett to include said second server computer is operative to provide facilities for storing and updating said network database in a manner that is visually consistent with a Web site on the first server as taught by Story for the purpose of maintaining consistency amongst company logos which are stored at a plurality of different web addresses [paragraph 53]. The skilled artisan would have been motivated to modify Nessett per the above such that company logos are consistent and thus easily recognizable by a visitor to a particular web site which includes the company logo.

Claim 2:

The combination of Nessett and Story discloses the elements of claim 1 as noted above and furthermore, Nessett discloses wherein said second server computer comprises a server computer operative to store and update a network database [col 15, lines 55-65].

Claim 3:

The combination of Nessett and Story discloses the elements of claim 1 as noted above and furthermore, Nessett discloses wherein said first server computer comprises a server computer operative to provide an Internet Web site [Fig 2, and col 15, lines 40-47]

Claim 5:

The combination of Nessett and Story discloses the elements of claim 1 as noted above and furthermore, Nessett discloses receiving an indication that access to said second server computer may be granted, redirecting said user from said first computer to said second computer [servers cooperate to grant the user admittance to both servers, col 15, lines 55-65].

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Pat No 5,968,176 issued to Nessett et al (hereafter Nessett) in view of US Pat No 6,539,021 issued to Kennelly et al (hereafter Kennelly).

Claim 9:

Nessett discloses the elements of claims 6-8 as noted above but does not disclose determining whether said new user has been previously been added to said group of users authorized to utilize said network database and in response to determining that said user has previously been added to said group of authorized users, denying said request to add said new user. Kennelly discloses determining whether said new user has been previously been added to said group of users authorized to utilize said network database and in response to determining that said user has previously been added to said group of authorized users, denying said request to add said new user [Fig 8, col 10, line 65 - col 11, line 5, checks user identification and password against the level of security access privileges of the user , in this case authentication is valid and the parser is established for the session]. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nessett to include determining whether said new user has been previously been added to said group of users authorized to utilize said network database and in response to determining that said user has previously been added to said group of authorized users, denying said request to add said new user as taught by Kennelly for the purpose of preventing duplicate log-in entries for the user. The skilled artisan would have been motivated to modify Nessett per the above such that the access control list for the user group would not be confused by duplicate entries for the users registered in the group.

Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in view of US Pat No 6,339,826 issued to Hayes et al (hereafter Hayes).

Claim 11:

Nessett discloses a method for providing remote access to the facilities of a server computer, comprising:

receiving a request at a server computer operative to store and update a network database to update user data for a user authorized to utilize said network database; determining whether said request may be granted; and in response to determining that said request may be granted, updating said user data as specified in said request [Fig 2 and col 16, line 55 – col 17, line 3].

Nessett discloses the elements of the claimed invention as noted above but does not disclose the user being removable from the server computer when a corresponding user is removed from another server computer that issues the request. Hayes discloses the user being removable from the server computer when a corresponding user is removed from another server computer that issues the request [col 21, lines 15-32, Fig 22, administrator has Add/Remove group membership buttons]. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nessett to include the user being removable from the server computer when a corresponding user is removed from another server computer that issues the request as taught by Hayes for the purpose of adding/deleting users from the group. The skilled artisan would have been motivated to modify Nessett per the such that the dynamic situation in the business world can be accommodated wherein employees are constantly being assigned to and removed from groups.

Claim 12:

The combination of Nessett and Hayes discloses the elements of claim 11 as noted above and furthermore, Nessett discloses wherein said request is received over a secure communications link from a second server computer [col 16, lines 13-20].

Claim 13:

The combination of Nessett and Hayes discloses the elements of claim 11 as noted above and furthermore, Nessett discloses wherein said first server computer comprises a server computer operative to provide an Internet Web site [Fig 2, and col 15, lines 40-47]

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in view of US Pat No 5,946,686 issued to Schmuck et al (hereafter Schmuck).

Claim 14:

Nessett discloses:

receiving a request [Fig 2, 111] for a facility available at a server computer operative to store and update a network database via a secure communications link [Fig 2];

determining whether said request may be granted [col 15, lines 55-65];

in response to determining that said request may be granted, executing said facility at said server computer according to said request [Fig 2, col 15, lines 55-65 and col 16, lines 13-20].

Nessett discloses the essential elements of the claimed invention as noted above but does not disclose said facility including creation of a new collaborative group in which users may share data, the method refraining from creating said collaborative group if a quota has been exceeded. Schmuck discloses said facility including creation of a new collaborative group in which users may share data [col 4, lines 63-67]. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nessett to include said facility including creation of a new collaborative group in which users may share data as taught by Schmuck for the purpose of regulating a user/ user group according to the amount of disk space that is available [col 4, lines 63-67]. The skilled technician would have been motivated to modify Nessett per the above such that a shared disk file system running on multiple computers can be coupled for parallel data sharing access to files residing on network shared disks [abstract].

Claims 15, 16 and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Nessett and Schmuck and further in view of Hayes.

Claims 15 and 21:

The combination of Nessett and Schmuck discloses the elements of claim 14 as noted above but does not disclose the user being removable from the server computer when a corresponding user is removed from another server computer that issues the request. Hayes discloses the user being removable from the server computer when a corresponding user is removed from another server computer that issues the request [col 21, lines 15-32, Fig 22]. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Nessett and Schmuck to include the user being removable from the server computer when a corresponding user is removed from another server computer that issues the request as taught by Hayes for the purpose of adding/deleting users from the group. The skilled artisan would have been motivated to modify the combination of Nessett and Schmuck per the above such that the dynamic situation i the business world can be accommodated wherein employees are constantly being assigned to and removed from groups.

Claim 16:

The combination of Nessett, Schmuck and Hayes discloses the elements of claims 14 and 15 as noted above and furthermore, Nessett discloses wherein said request further comprises a user ID for said user to be deleted [col 12, lines 10-21]

Claim 19:

The combination of Nessett, Schmuck and Hayes discloses the elements of claim 14 as noted above and furthermore, Nessett discloses wherein said request further comprises the identity of one or more users to be added to said new collaborative group [col 16, line 55-col 17, line 3].

Claim 20:

The combination of Nessett, Schmuck and Hayes discloses the elements of claim 14 as noted above and furthermore, Nessett discloses wherein said facility comprises an application programming interface for adding new users to an existing collaborative group in which users may share data [col 16, line 55-col 17, line 3].

(10) Response to Argument

Claim Rejection Withdrawn:

Claims 11-13 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 11 recites "the user being removable from the server computer when a corresponding user is removed from another server computer that issues the request." The skilled artisan would not be able to make and use the invention because the specification does not contain a clear and concise description of what comprises a "corresponding user" and also does not include a clear and accurate description of why a corresponding user must be removed before "the user" is removable.

Appellant on page 7 of the Appeal Brief indicates that support for above claim limitation is found on page 3, lines 13-27 which is reproduced below.

More specifically described, a login user servlet is provided for receiving requests to authorize a user to access the co-branded Web site and for validating such requests. Through the use of the login user servlet, a user may be concurrently logged in to the co-branded Web site and a partner Web site. A create servlet and a delete user servlet are provided for authorizing new users to access the co-branded Web site or deleting user authorization for accessing the co-branded Web site, respectively. A create webgroup servlet is provided for creating a new webgroup through which users may collaborate and share resources over a network communications link. Moreover, servlets are also provided for adding users to a list of users authorized to access the webgroup and for removing users from the list of users authorized to access the webgroup. Still further, servlets are provided for issuing an invitation to join the co-branded Web site to a user that has not joined the co-branded Web site. Additionally, a servlet is provided for issuing an invitation to join the co-branded Web site to a user that previously received such an invitation, but lost the previously issued invitation.

In light of the specification examiner will interpret the claim language "said user being removable from the server computer when a corresponding user is removed from another server computer that issues the request" to mean that a new user can be added to the group and an existing member of the group can be deleted.

Claim 1:

Appellant maintains on page 24 of the Appeal Brief that regarding claim 1, the combination of Nessett and Story does not disclose "said second server computer is operative to provide facilities for storing and updating a network database in a manner that is visually consistent with a Web site on said first server computer."

Examiner is not persuaded for the following reasons. **Appellant** (emphasis added) states on page 5 of the Appeal Brief that the following excerpt from the specification, i.e., page 27, lines 26-29 supports above limitation:

In order to provide a version of the Webgroups WWW site that is user-friendly, the co-branded version of the WebGroups WWW site may be provided in a manner that is visually consistent with a business partner website provided by the business partner.

Examiner has correctly interpreted the claim language "in a manner that is visually consistent" to mean the presence of the company logo on two or more websites per the following disclosure by Story.

Story discloses the following in paragraph 53:

[0053] Another preference option allows an author to specify a linked document as a Trusted Reference 94. As noted above, documents copied into the Stage Subdirectory 64 eventually may be distributed to a directory on a network server 62. In some cases, an author may be confident that a specific sublevel document exists already on the network server 62 and may wish that document to be referenced at its existing address on the network rather than creating a duplicate locally. **For example, Silicon Graphics, Inc. may have multiple hypermedia documents published in directories on a specific network server at http://www.sgi.com/websites, and may have a logo directory on that server at http://www.sgi.com/websit- es/logos, which includes image documents corresponding to logos for its various products. So that the logos are used consistently in its hypermedia documents, the company may desire that each hypermedia document references the documents in the logo directory rather than referencing image documents stored at other addresses**. In such a case, an author of a company hypermedia document that includes links to image documents for logos may specify linked documents at http://www.sgi.com/websites/logos as Trusted References. Not only does this practice ensure that shared documents are consistent, but it also saves space and reduces subsequent maintenance work, often to a substantial degree.

Story discloses a network database (logo directory) of image documents corresponding to logos for its various products. Each hypermedia document[1] references the logo directory such that each hypermedia document incorporates the authorized and registered company logo which is well-known and easily recognized by a visitor to one of the websites which includes one or more of the company's products. Story discloses that each and every hypermedia document when published on the world wide web is made visually consistent by including a company-authorized logo.

The disclosure of Story reads on the claim limitation "in a manner that is visually consistent with a Web site on said first server computer."

Claims 2, 3 and 5:

Appellant maintains on page 24 of the Appeal Brief that the combination of Nessett and Story does not read on the claim limitation(s). Examiner is not persuaded for the reasons given below.

Regarding claim 2, examiner is not persuaded because Nessett discloses said second server computer comprises a server computer operative to store and update said network database. Nessett discloses the following in column 14, line 63 through column 15, line 20:

There are two major applications of Access Server equipment. The first is to provide remote access to private intranets. In such cases the Access Server is located within the private intranet, allowing remote access by stand-alone end systems and remote office routers through the PSTN. The second application of remote access products is within Internet Service Provider (ISP) networks. These give subscribers access to the ISP content equipment as well as the ISP's Internet connections. These two applications have somewhat different security requirements, which are discussed in more detail below.

79

[1] Hypermedia is defined as the combination of text, video, graphic images, sound, hyperlinks, and other elements in the form typical of web documents. Essentially hypermedia is the modern extension of hypertext, the hyperlinked, text-based documents of the original Internet. Microsoft Computer Dictionary, Fifth Edition.

The two functions of remote access equipment, line servicing and packet processing, are traditionally implemented within the same chassis. Recent changes in customer requirements, specifically the desire to use public WANs to implement Private Virtual Networks, has led vendors to separate these functions into two different products, the line server and the packet server. When customers use these products, the line server is connected on one side to the PSTN (or perhaps directly to end systems) and on the other side to a WAN. The packet server is connected on one side to a private intranet or ISP facility, and on the other side to the WAN. For each connection, the line server creates a protected tunnel through the WAN (normally using cryptographic technology) to the packet server. Connections to the line server may come either from stand-alone end systems or from remote office routing equipment.

From the above disclosure by Nessett it can be seen that irrespective of whether the line server 104 or the packet server 108, is designated respectively a first server or a second server, both servers include a database by virtue of the fact that the servers provide remote access to private intranets and to Internet Service Provider (ISP) networks. Providing access control includes maintaining at least as access control list of subscribers authorized to access the server. The access control list reads on the claimed database.

Regarding claim 3, Nessett discloses a Web site [col 4, lines 20-45 teaches nodes distributed on a network such as the Internet Protocol IP layer].

Regarding claim 5, Nessett discloses "receiving an indication that access to said second server computer should also be granted, redirecting said user from said first computer to said second computer [col 15, lines 55-65 discloses split service access which requires two network access control decisions. The first allows a user access to the line server and the second allows him access to the packet server]

Claim 6:

Appellant maintains regarding claims 6, 22 and 23 on page 17 of the Appeal Brief that Nessett does not disclose "adding said new user to said group of users authorized to utilize said network database, said group of users defining a collaborative group spanning across said server computer and another server computer so as to allow users to share data."

Examiner is not persuaded. Nessett discloses the following in column 8, lines 1-15:

The generic term "node" refers to either end systems or network devices. End systems (aka hosts) are the nodes identified in policy statements. A special case occurs, for example, when a network device is accessed for management purposes. In this case the network device acts in the role of an end system. End systems in the network may belong to groups. Groups are named and their membership is established by input to the security policy language front end by a system administrator or otherwise, or in the alternative implemented in the topology data base. Again this input can occur either by user interface interactions or by the security policy language front end reading files or other data bases. Groups of end systems may be specified as containing individual end systems or other groups of end systems.

Furthermore, Nessett discloses the following in column 16, line 60 through column 17, line 5 the following:

In general, part of this activity is centrally administered and part is left to a user's discretion. So, access control to group membership is a two step process. In the first step, a system administrator forms the group and establishes the policy by which users or systems may join it. In the second step, a user decides to join the group or decides to place a system in the group. The access control machinery than consults the policy data associated with the group and determines whether the proposed membership request is valid. Each step of this access control decision must be secure.

Nessett discloses that a user can be admitted to a user group to share a database system with the group. Nessett discloses the group can extend over a network comprising nodes or hosts. Nessett reads on the claim limitation "adding said new user to said group of users authorized to utilize said network database, said group of users defining a collaborative group spanning across said server computer and another server computer so as to allow users to share data."

Claim 9:

Appellant maintains regarding claim 9 on page 27 of the Appeal Brief that the combination of Nessett and Kennelly does not disclose "determining whether said new user has previously been added to said group of users authorized to utilize said network database and in response that said new user has previously been added to said group of authorized users, denying said request to add said new user." Examiner is not persuaded for the reasons given below.

The above limitation(s) need to be interpreted according to the specification. In the Appeal Brief on page 7, Appellant points to page 36 line 21 of the specification which states "The Routine 2500 then continues to block 2520, where an electronic message is transmitted to the new user with notification that the user has been added to the new webgroup." The essence of the claim limitation is that a new user can be added to a workgroup. The specification is silent regarding denying access. Nessett discloses the following in column 16, lines 55-65:

Two network management problems are characterized by significant security issues. The first is network management security, that is, ensuring the network management subsystem is not subverted. An important issue is how to implement securely VLAN, VNET, or other group formation, which is an access control function. In general, part of this activity is centrally administered and part is left to a user's discretion. So, access control to group membership is a two step process. **In the first step, a system administrator forms the group and establishes the policy by which users or systems may join it. In the second step, a user decides to join the group or decides to place a system in the group.** The access control machinery then consults the policy data associated with the group and determines whether the proposed membership request is valid. Each step of this access control decision must be secure.

Kennelly discloses the following in column 10,line 65 through column 11, line 5:

If the user has not logged in previously, the management object request processor 156 requests the user identification and password. The request processor 156 interfaces with the security object 201 (FIG. 7) to verify the login information. The security object 201 (FIG. 7) checks the user identification and password against the level of security access privileges of the user. If the **information is invalid, the switch 12 prompts the user to enter valid information.**

Nessett discloses the formation of a new user group and Kennelly discloses denying access if the user entered information is invalid and further prompting the user to enter valid information. The combination of Nessett and Kennelly discloses above claim limitation **as interpreted according to the specification** (emphasis added) that a new user can be added to the workgroup.

Claim 10:

Appellant maintains on page 23 of the Appeal Brief that Nessett does not disclose "wherein said server computer comprises a server computer operative to store and update a network database, and wherein said second server computer comprises a server computer operative to provide an Internet Web site. Examiner is not persuaded for the following reasons.

Nessett discloses a Web site [col 4, lines 20-45 teaches nodes distributed on a network such as the Internet Protocol IP layer.

Claim 11:

Appellant maintains the combination of Nessett and Hayes does not disclose "said user being removable from the server computer when a corresponding user is removed from another server computer that issues the request."

Examiner is not persuaded. Examiner maintains the specification lacks written description to provide support for above claim language.

Appellant on page 3 of the Appeal Brief points to page 3, lines 21-23 of the specification for interpretation of above claim language.

Moreover, servlets are also provided for adding users to a list of users authorized to access the webgroup and for removing users from the list of users authorized to access the webgroup.

Hayes discloses the following in column 21, lines 15-32:

FIG. 22 shows the right panel when the administrator selects the second tab "Group Memberships". List 2220 shows all subgroups of which colleend is a member. The subgroups are shown in this list in the order of subgroup priority for colleend. The administrator can change colleend's subgroup priority by selecting a subgroup and using the up and down arrows to the right of list 2220 to move the selected subgroup up or down the list as desired. If the administrator clicks the **"Add/Remove Group Memberships"** button 2242 in FIG. 22, the right panel then shows the contents of FIG. 23. The FIG. 23 right panel allows the administrator to modify the subgroups of which colleend is a member. The administrator does this by clicking on an appropriate box corresponding to a desired subgroup. If the box is clear (meaning that colleend is not presently a member), then a check mark is added to the box to include colleend in the subgroup. Conversely, if a subgroup box is already checked, then clicking on the box clears the check mark and removes colleend from the subgroup.

Hayes clearly reads on the claim limitation "said user being removable from the server computer when a corresponding user is removed from another server computer that issues the request" when the claim limitation is interpreted according to the specification. The specification merely describes a user being removed from a list of users. Hayes clearly discloses a user being removed from a group of authorized users.

Claim 12:

Appellant maintains on page 31 of the Appeal Brief that the combination of Nessett and Hayes does not disclose "wherein said request is received over a secure communications link from a second server computer." Examiner is not persuaded for the reason(s) given below.

Nessett discloses the following in column 16, lines 13-20:

Finally, protected communications is an important service provided by Remote Access. This may occur in two places. In some situations, the physical security provided by the PSTN may be insufficient to provide appropriate guarantees to the user/Private Intranet. In such cases, the

Modem/Remote Access Router may **cryptographically protect its communications with the Access/Line Server. This requires cryptographic protocols that run over serial lines.**

Nessett discloses above limitation.

Claim 13:

Appellant on page 32 of the Appeal Brief maintains that the combination of Nessett and Hayes does not disclose "wherein said server computer comprises a server computer operative to store and update a network database and wherein said second server computer comprises a server computer operative to provide an Internet Web site." Examiner is not persuaded for the reasons given below.

Nessett discloses a Web site [col 4, lines 20-45 teaches nodes distributed on a network such as the Internet Protocol IP layer.

Claim 14:

Appellant on page 33 of the Appeal Brief maintains the combination of Nessett and Schmuck does not disclose "the method refraining from creating said collaborative group if a quota has been exceeded." Examiner is not persuaded. Schmuck discloses the following in column 4, lines 63-67:

As a quota is a limit on the amount of disk that can be used by a user or group of users, in order to use the concept in our parallel file system, we have created a way for local shares to be distributed by a quota manager (which accesses the single quota file) for parallel allocation.

Furthermore, Schmuck discloses the following in column 45, lines 20-30:

The quota server gives out local shares as long as it still has quota available, i.e., the system wide quota limit is not exceeded. If all of the quota limit has been given as local shares, the quota server will revoke local shares to satisfy new requests. This will be done by revoking part of the local shares allowing the client to continue using the remaining share. These requests will become stronger revoking larger portions of local shares until no quota is available to satisfy requests **causing application requests to be denied**.

Schmuck clearly reads on the claim limitation "refraining from creating said collaborative group if a quota has been exceeded."

Claims 15, 19, 20 and 21:

Appellant maintains on page 35 of the Appeal Brief that the combination of Nessett, Schmuck and Hayes does not disclose the limitations of above claims. Examiner is not persuaded for the following reasons:

Regarding claim 15, Hayes discloses the claim limitation "wherein said facility comprises an application programming interface for deleting access rights for a user to said server computer."

Hayes discloses the following in column 21, lines 15-32:

FIG. 22 shows the right panel when the administrator selects the second tab "Group Memberships". List 2220 shows all subgroups of which colleend is a member. The subgroups are shown in this list in the order of subgroup priority for colleend. The administrator can change colleend's subgroup priority by selecting a subgroup and using the up and down arrows to the right of list 2220 to move the selected subgroup up or down the list as desired. If the administrator clicks the **"Add/Remove Group Memberships"** button 2242 in FIG. 22, the right panel then shows the contents of FIG. 23. The FIG. 23 right panel allows the administrator to modify the subgroups of which colleend is a member. The administrator does this by clicking on an appropriate box corresponding to a desired subgroup. If the box is clear (meaning that colleend is not presently a member), then a check mark is added to the box to include colleend in the subgroup. Conversely, if a subgroup box is already checked, then clicking on the box clears the check mark and removes colleend from the subgroup.

Hayes clearly teaches above claim limitation.

Regarding claim 19, Nessett discloses wherein said request comprises the identity of one or more users to be added to said new collaborative group." Nessett discloses the following in column 16, line 60 through column 17, line 5 the following:

In general, part of this activity is centrally administered and part is left to a user's discretion. So, access control to group membership is a two step process. In the first step, a system administrator forms the group and establishes the policy by which users or systems may join it. In the second step, a user decides to join the group or decides to place a system in the group. The access control machinery than consults the policy data associated with the group and determines whether the proposed membership request is valid. Each step of this access control decision must be secure.

Nessett clearly discloses above limitation.

Regarding claim 20, Nessett discloses wherein said facility comprises an application programming interface for adding new users to an existing collaborative group in which users may share data. Nessett discloses the following in column 16, line 60 through column 17, line 5 the following:

In general, part of this activity is centrally administered and part is left to a user's discretion. So, access control to group membership is a two step process. In the first step, a system administrator forms the group and establishes the policy by which users or systems may join it. In the second step, a user decides to join the group or decides to place a system in the group. The access control machinery than consults the policy data associated with the group and determines whether the proposed membership request is valid. Each step of this access control decision must be secure.

Nessett clearly discloses above limitation.

Regarding claim 21, Nessett discloses "wherein said facility comprises an application programming interface for removing users from an existing collaborative group in which users may share data." Nessett discloses the following in column 16, line 60 through column 17, line 5 the following:

In general, part of this activity is centrally administered and part is left to a user's discretion. So, access control to group membership is a two step process. In the first step, a system administrator forms the group and establishes the policy by which users or systems may join it. In the second step, a user decides to join the group or decides to place a system in the group. The access control machinery than consults the policy data associated with the group and determines whether the proposed membership request is valid. Each step of this access control decision must be secure.

Nessett clearly discloses above limitation.

Claim 16:

Appellant maintains on page 16 of the Appeal Brief that the combination of Nessett, Schmuck and Hayes does not disclose "wherein said request further comprises a user ID for said user to be deleted." Nessett discloses the following in column 12, lines 10-21:

Both NICs and modems can provide features that support network access control. Modems may require a user to provide a password, use a token card or otherwise provide proof that he is authorized to initiate a connection before performing the out-dialing sequence. Modems also may support callback functionality in Access Servers that only allow connections from authorized phone numbers.

Nessett clearly discloses above limitation.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Conferees:

John E. Breene

John Breene

SPE Tech Center 2100

Apu Mofiz

SPE Tech Center 2100

Etienne P. LeRoux

Etienne LeRoux

Primary Examiner AU 2161